(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２００２－８２９１１
（Ｐ２００２－８２９１１Ａ）
(43)公開日　平成14年3月22日(2002.3.22)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｃ	5B035
					３３０Ｇ	5B058
		ＺＥＣ			ＺＥＣ	5B085
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｌ	5J104
	19/10			19/00	Ｒ	

審査請求　有　請求項の数７　ＯＬ　（全６頁）　最終頁に続く

(21)出願番号　特願2000-274421(P2000-274421)

(22)出願日　平成12年9月11日(2000.9.11)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者　諏訪本　剛
東京都港区芝五丁目7番1号　日本電気株式会社内

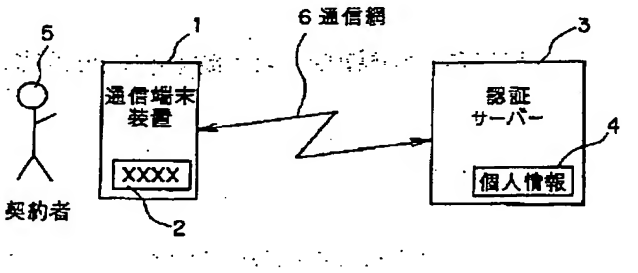
(72)発明者　大沢　一秋
東京都港区芝五丁目7番1号　日本電気株式会社内

(74)代理人　100071526
弁理士　平田　忠雄

最終頁に続く

(54)【発明の名称】認証システム

(57)【要約】
【課題】　セキュリティを確保しながら利用者を煩わせることなく、セキュリティ対策のための費用を低減することが可能な認証システムを提供する。
【解決手段】　通信端末装置１には製造時に付けられた固有のＩＤ２を有し、通信網６を介して通信端末装置１に接続された認証サーバー３には、個人情報４が登録されている。通信端末装置１から接続要求があったとき、認証サーバー３から通信端末装置１にＩＤ２の送信を要求する。認証サーバー３は、通信端末装置１からのＩＤ２の照合により認証を行い、認証ＯＫのときにサービスを可能にする。



【特許請求の範囲】

【請求項１】　利用者が希望するサービスの提供を通信回線又はネットワークに接続されている端末装置を介して行うに際し、前記利用者が真正であるか否かの認証を行う認証システムにおいて、
前記通信回線又は前記ネットワークに認証用の個人情報が登録された認証サーバーを接続し、
前記端末装置から接続要求があったとき、前記認証サーバーから前記端末装置に付けられた固有のＩＤの送信を要求し、受信した前記ＩＤの照合の可否により認証を行うことを特徴とする認証システム。

【請求項２】　前記固有のＩＤは、前記端末装置の製造時に設定ならびに記憶することを特徴とする請求項１記載の認証システム。

【請求項３】　前記端末装置は、携帯電話機、簡易型携帯電話機（ＰＨＳ）、ＰＤＡ（Personal Digital Assistant）端末装置、又はセットトップボックスであることを特徴とする請求項１記載の認証システム。

【請求項４】　前記固有のＩＤは、前記端末装置に着脱可能なＩＣカードに設けられていることを特徴とする請求項１記載の認証システム。

【請求項５】　前記認証サーバーは、前記端末装置からのパスワードの入力を認証条件の１つにすることを特徴とする請求項１記載の認証システム。

【請求項６】　前記認証サーバーは、前記端末装置からのアクセスを受け付ける処理、前記端末装置に前記固有のＩＤの送信を要求する処理、及びウェブサーバーとの通信を行う処理を担当するエージェントが接続されていることを特徴とする請求項１又は５記載の認証システム。

【請求項７】　前記エージェントは、電子ショッピングを実行するための買物エージェントであり、
前記ウェブサーバーは、商品販売店に設置されていることを特徴とする請求項６記載の認証システム。

【発明の詳細な説明】

【０００１】本発明は、認証システムに関し、特に、通信端末装置を用い、通信回線（ネットワーク）を通して電子ショッピング等を行う際の利用者の情報漏洩を防止するための認証システムに関する。

【０００２】

【従来の技術】従来、通信端末装置を用いた電子ショッピングは、商品購入の都度、利用者がクレジットカードの番号或いは個人情報（住所、氏名、銀行口座番号など）を通信端末装置からネットワークに接続されたホストコンピュータに通知する方式が用いられている。また、ＬＡＮ（Local AreaNetwork）などでは、ＩＤ（IDentification）やパスワード（password）等の利用者識別子を設定し、利用者が適正なアクセス者であるか否かを認証している。この場合、外部の第三者による不正アクセスの防止は、情報が外部に漏れないようにするために必須である。この対策については、例えば、特開２０００－１０９２７号公報に提案がある。

【０００３】特開２０００－１０９２７号公報においては、予め認証装置に利用者の「利用者ＰＨＳ番号」、「認証装置パスワード」、「リモート接続ＩＤ」を登録しておき、利用者が「認証装置電話番号＋認証装置パスワード」による回線接続に対し、「利用者ＰＨＳ番号」と「認証装置パスワード」を確認し、これらが合致するときに利用者のＰＨＳ端末機に対して一時的なパスワードを発行する旨、及び利用者ＰＨＳ端末機の通信を一旦オフにして待ってほしい旨のメッセージを通知する。認証装置は利用者に対して一時的なパスワードを発行し、利用者のＰＨＳ端末機に文字メッセージで表示させる。利用者は、一時的なパスワードを用いてパーソナルコンピュータ（ＰＣ）とリモート接続装置を接続することにより、ネットワークサービスを受けることが可能になる。

【０００４】

【発明が解決しようとする課題】しかし、従来の認証システムによれば、利用者がクレジットカード番号或いは個人情報を入力して利用者の識別を行った場合、クレジットカード番号や個人情報のなりすましが可能であり、セキュリティ上で問題が発生する可能性がある。また、利用者は情報の入力操作を強いられるという面倒がある。

【０００５】また、特開２０００－１０９２７号公報によれば、ＰＨＳ端末機を所持していなければ一時的なパスワードを取得できず、また、所持していても回線接続及び一時的なパスワードの入手作業が要求され、利用者にとっては煩わしい。

【０００６】したがって、本発明の目的は、セキュリティを確保しながら利用者を煩わせることなく、セキュリティ対策のための費用を低減することが可能な認証システムを提供することにある。

【０００７】

【課題を解決するための手段】本発明は、上記の目的を達成するため、利用者が希望するサービスの提供を通信回線又はネットワークに接続されている端末装置を介して行うに際し、前記利用者が真正であるか否かの認証を行う認証システムにおいて、前記通信回線又は前記ネットワークに認証用の個人情報が登録された認証サーバーを接続し、前記端末装置から接続要求があったとき、前記認証サーバーから前記端末装置に付けられた固有のＩＤの送信を要求し、受信した前記ＩＤの照合の可否により認証を行うことを特徴とする認証システムを提供する。

【０００８】このシステムによれば、端末装置に固有のＩＤと個人情報をサーバ側でデータベース化しておき、利用者が端末装置を接続した際、サーバ側から端末装置にＩＤを送信するように要求し、このＩＤの照合結果に

基づいて認証を実施する。したがって、利用者による認証のための入力操作を不要にできるので、個人情報等が第三者に知られるのを防止できる（セキュリティを確保できる）。また、入力操作を要求されることがないので、利用者を煩わせることがない。さらに、一時的なパスワードを発行する必要がないので、セキュリティ対策のための費用を低減することができる。

【０００９】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。

〔第１の実施の形態〕図１は本発明の認証システムを示す。１台毎に固有のＩＤ２が設定された通信端末装置１には、通信網６を介して認証サーバー３が接続されている。認証サーバー３にはＩＤ２が登録されており、さらにＩＤ２に関連付けられた個人情報４が格納されている。ＩＤ２は、製造メーカーにおいて製造時に付けられる複数桁の数字、又は数字と英字の組み合わせ等による固有のもの（製品シリアルナンバーとは異なる）で、管理者等が再設定や変更を行うことは不可能であり、同じ内容により他の通信端末装置に再使用され得ない固定されたものである。したがって、極めて識別度及び安全性の高いＩＤが得られる。このＩＤ２は、例えば、電子ショッピングに加入する際、管理者側に設置された専用の入力機器により読み出され、個人情報４と共に認証サーバー３に記憶される。個人情報４には、住所、氏名、銀行口座番号、信用情報等が用いられる。この個人情報４によって、通信端末装置１を用いて行われる通信サービスの契約者５が特定される。ＩＤ２と個人情報４が対応しているので、ＩＤ２から個人情報４が検索される。

【００１０】通信端末装置１には、ＪＡＶＡ（ジャバ）仮想マシン（Java Virtual Machine）の機能を備えたものを用いる。ＪＡＶＡ仮想マシンは、米国のSun Microsystems社によって開発されたプログラミング言語であるＪＡＶＡを用いて構築されたマシンであり、Ｗｉｎｄｏｗｓ（登録商標）やＵｎｉｘ等のＯＳ上で動作する。このような通信端末装置１として、携帯電話機、簡易型携帯電話機（ＰＨＳ：PersonalHandyphone System）、通信機能を備えたＰＤＡ（Personal Digital Assistant）装置、セットトップボックス（ＳＴＢ）等があるが、上記したように、製造段階で固有のＩＤ２が設けられていることが条件になる。

【００１１】図１の構成において、認証サーバー３には、予め契約者５の個人情報４が登録されている。契約者５は、通信端末装置１を認証サーバー３に接続したいとき、認証サーバー３の呼び出しを行う。この呼び出しに対し、認証サーバー３は通信端末装置１に対してＩＤ２の送信を要求する。通信端末装置１は、認証サーバー３の要求に応じてＩＤ２を認証サーバー３へ送出する。認証サーバー３は、取得したＩＤ２が認証サーバー３に登録されているＩＤの中に一致するものがあるか否かを照合する。照合できた場合、一致したＩＤ２に対応した個人情報４を用いて電子ショッピングの処理を実行する。

【００１２】このように、通信端末装置１に個別に設定された固有のＩＤ２を用いて認証を行うことにより、個人情報を通信端末装置１からキー入力する必要が無くなるので、個人情報のセキュリティを確保することができる。また、個人情報を入力する必要が無いので、煩わしさを感じさせることもない。

【００１３】〔第２の実施の形態〕上記したように、本発明は、通信端末装置１毎に設けられているＩＤを用いて一義的に認証を行っているため、通信端末装置１が盗難等により他人の手に渡ってしまった場合、第三者に利用されてしまう恐れがある。そこで、第２の実施の形態では、パスワードの入力を義務付けるものとする。このパスワードは、個人情報として予め登録したものを用いる。

【００１４】図２は本発明による認証システムの実施例を示す。本実施例は、電子ショッピングを行うためのネットワークシステムの一例を示す。図２においては、図１に示したと同一の構成又は機能を有するものには、同一引用数字を用いている。また、図１の通信端末装置１として、携帯電話機、ＰＨＳに代表される携帯端末装置１０を用いている。携帯端末装置１０は、上記したように、内部に通信端末固有のＩＤ２を有しており、通信網６の加入者（契約者）の端末の位置付けにある。携帯端末装置１０を使った通信サービスの契約者が契約者５である。通信網６には、認証サーバー３が接続された買物エージェント（agent ）８と各商品販売店に設置されたＷｅｂ（ウェブ）サーバー（Web server）７が接続されている。認証サーバー３には、認証を行うための個人情報（住所、氏名、銀行口座番号、信用情報等）４が格納されており、一種のデータベースとして機能している。買物エージェント８は、電子ショッピングの要求を受けると起動し、内蔵する知識ベースに基づいて電子ショッピングに関する様々な処理を自律的に実行する機能を備えている。

【００１５】図３は図２のシステムの動作を示す。また、図４は買物エージェント及び認証サーバーにおける処理を示す。図３及び図４を用いて、図２の構成の動作について説明する。以下において、図中のＳはステップを表している。契約者５が電子ショッピングを行う場合、携帯端末装置１０を用い、通信網６を介して買物エージェント８に接続する（Ｓ１０１、Ｓ２０１）。買物エージェント８は、携帯端末装置１０の識別を行うため、ＪＡＶＡアプレット（ＪＡＶＡ言語をベースにして記述され、ブラウザ内で動作するプログラム）を用いて携帯端末装置１０にＩＤ２の送信要求を行う（Ｓ１０２、Ｓ２０２）。この要求に対し、携帯端末装置１０はＩＤ２を買物エージェント８に送信する（Ｓ１０３）。

買物エージェント８は、ＩＤ２を受信すると（Ｓ２０３）、これを認証サーバー３に送る。認証サーバー３は、ＩＤ２と事前に登録されている個人情報４により認証を行い（Ｓ１０４、Ｓ２０４）、認証が成立（Ｓ２０５）したときにはＷｅｂサーバー７に通知する（Ｓ１０５、Ｓ２０６）。

【００１６】買物エージェント８からのＩＤ２の送信要求に対し、所定時間が経過してもＩＤ２が送られてこなかった場合、及び、認証サーバー３による認証が不成立のときには、通信を拒絶する処理を実行する（Ｓ１０６、Ｓ２０８）。認証の成立時、Ｗｅｂサーバー７は、通信網６及び買物エージェント８を通して（Ｓ１０７）携帯端末装置１０との接続を行い（Ｓ１０８）、携帯端末装置１０とＷｅｂサーバー７の相互間で通信が行われる（Ｓ１０９、Ｓ１１０）。契約者５はＷｅｂサーバー７との間で必要な手続きを行えば、所望の商品を購入することができる。

【００１７】以上のように、本発明の実施例によれば、携帯端末装置１０に個別に設定された固有のＩＤ２を用いて認証を行うことにより、個人情報を携帯端末装置１０からキー入力する必要が無くなるため、個人情報のセキュリティを確保することができる。また、個人情報を入力する必要が無いため、煩わしさが無くなる。

【００１８】また、携帯端末装置１０のＩＤ２として、携帯端末装置１０の内部にＩＤが記憶されている形態のほか、ＩＣカードにＩＤ２を記憶させておき、このＩＣカードを携帯端末装置１０に組み込む構成にしてもよい。さらに、上記実施の形態においては、電子ショッピングについて説明したが、本発明は電子ショッピングに限定されるものではなく、不特定多数の人が利用するインターネットや電話回線等を用い、その際に個人情報が取り扱われる全ての通信（インターネット通販、電子商取引等）に適用可能である。

【００１９】

【発明の効果】以上説明した通り、本発明の認証システムによれば、端末装置に固有のＩＤと個人情報をサーバ側でデータベース化しておき、利用者が端末装置を接続した際、サーバ側から端末装置にＩＤを送信するように要求し、このＩＤの照合結果に基づいて認証を行うようにしたので、利用者による認証のための入力操作が不要になり、個人情報等を第三者に知られるのを防止できる結果、セキュリティの確保が可能になる。また、入力操作を強いることがないので、利用者を煩わせることがない。さらに、一時的なパスワードを発行する必要がないので、セキュリティ対策のための費用を低減することができる。

【図面の簡単な説明】

【図１】本発明の認証システムを示すブロック図である。

【図２】本発明による認証システムの実施例を示すブロック図である。

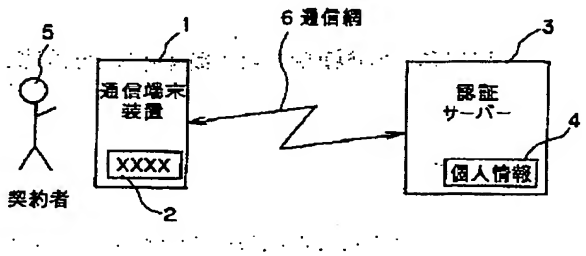
【図３】図２のシステムの動作を示すタイミングチャートである。

【図４】買物エージェント及び認証サーバーにおける処理を示すフローチャートである。

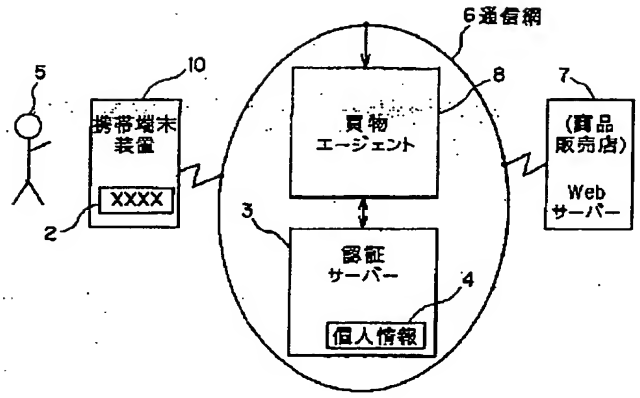
【符号の説明】

１　通信端末装置
２　ＩＤ
３　認証サーバー
４　個人情報
６　通信網
７　Ｗｅｂサーバー
８　買物エージェント
１０　携帯端末装置

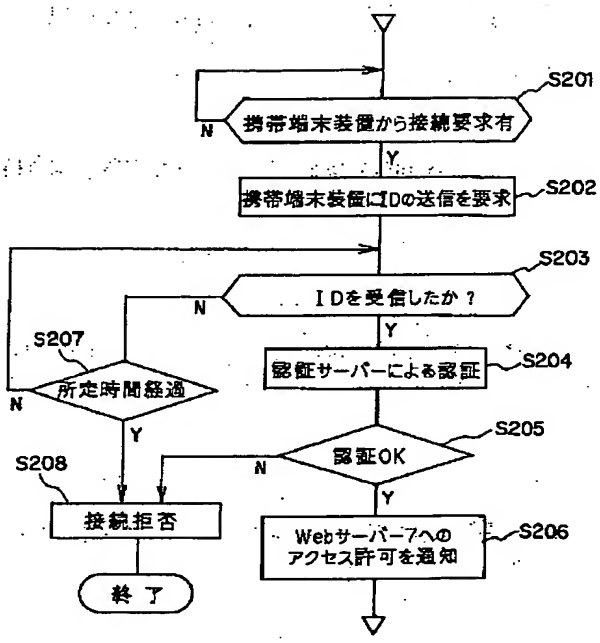
【図１】



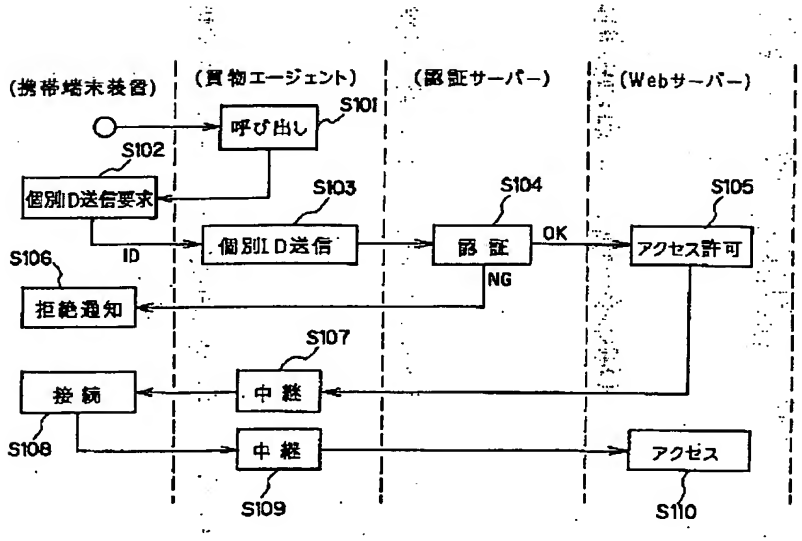
【図２】



【図４】



【図３】



フロントページの続き

(51) Int.Cl.⁷	識別記号	F I	テーマコード(参考)
H04L 9/32		H04L 9/00	673A
			673B
			673E

(72)発明者　佐藤　裕和
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　沼崎　武
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　田邉　泰祐
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B035 AA13 CA29
5B058 KA12 KA33
5B085 AE03 AE04 AE12 AE23 BG07
5J104 AA07 KA01 KA02 MA02 NA05
NA35 NA36 NA38 PA02 PA07